Keep up with Ransomware

해외 교육 기관을 노리는 FOG 랜섬웨어

■ 개요

2024 년 7 월 랜섬웨어 피해 사례는 전월(346 건) 대비 약 20% 증가한 415 건을 기록했다. 지난달 12 건의 피해자를 게시하며 주춤했던 LockBit 이 7 월에는 다시 33 건을 게시하며 활동량을 늘려가고 있다. 또한 자신들의 다크웹 유출 사이트에 연락 책임자로 추정되는 “Boss”의 메신저 ID 와 포럼 계정 등 연락 수단을 공개했다.

최근 특정 보안 제품의 기술적 문제에 대한 업데이트나 패치 파일로 위장해 사용자의 데이터를 삭제하는 Wiper 악성코드가 배포됐다. 7 월 19 일, 미국의 사이버 보안 기술 회사 크라우드스트라이크(CrowdStrike)의 차세대 엔드포인트 보안 플랫폼 팰컨(Falcon)에서 Windows 시스템 센서 구성 업데이트로 인해 시스템 충돌 및 블루스크린 증상이 발생해 업무가 마비되는 큰 파장이 있었다. 핵티비스트[1] 그룹 한다라(Handala)는 가짜 업데이트에 대한 설명과 지침이 담긴 PDF 파일을 배포했으며, 해당 문서 안에 업데이트 파일로 위장한 Wiper 를 다운로드 링크와 함께 기재해 Wiper 를 다운로드하도록 유도했다.

인도네시아의 국가 임시 데이터 센터를 공격한 브레인 사이퍼(Brain Cipher) 그룹은 7 월 3 일 자신들의 다크웹 유출 사이트에 복호화 키를 공개했다. 이들은 6 월 20 일 공격에 성공한 뒤 인도네시아 정부와 협상을 진행하며, 800 만 달러의 몸값을 요구한 것으로 알려졌다. 이들의 공격 동기는 정치적인 이유가 아닌 금전을 목적으로 한 침투 테스트였으며, 법 집행 기관의 압박 때문이 아니라 자발적으로 복호화 키를 공개한 것이라고 밝혔다. 추가로 이들은 앞으로는 절대로 대가 없이 복호화 키를 공개하지 않겠다고 언급했으며, 감사 표시의 기부는 받겠다며 암호 화폐 지갑 주소를 남기기도 했다.

[1] 핵티비스트: 해커(Hacker)와 액티비스트(Activist)의 합성어로 정치·사회적 목적으로 활동하는 해킹그룹을 뜻함

VMware ESXi[2] 서버를 주 타깃으로 하는 SEXi 랜섬웨어가 APT INC 로 이름을 변경하고 공격을 수행하고 있다. 이들은 유출된 Babuk 빌더[3]를 이용해 VMware ESXi 환경을 공격하고 LockBit 3.0 빌더를 이용해서 Windows 환경도 공격하는 것으로 확인됐다. 이외에도 여러 그룹이 ESXi 환경을 위협하고 있다. 6 월 25 일 출시된 ESXi 8.0 U3 버전의 인증 우회 취약점(CVE-2024-37085)을 이용해 공격자들이 전체 관리자 권한을 획득할 수 있었다. Storm-0506, Storm-1175, Octo Tempest, Manatee Tempest 로 알려진 그룹들이 취약점을 악용해 Akira 랜섬웨어와 BlackBasta 랜섬웨어를 배포했다.

해킹 포럼인 브리치포럼(BreachForums)에서 활동하는 인텔브로커(IntelBroker)가 한국 기관의 데이터를 판매하는 글 3 건을 게시했다. 기관 이름은 구체적으로 언급되지 않았으며, 각각 “Korean Policy Force”, “Korean Government Agency”, “Korean Critical Government Agency”로 기재했다. IntelBroker 가 판매하는 데이터에는 관리자 포털이나 접근 권한, 중요 문서 등이 포함되어 있지만, 샘플을 공개하면 바로 보안 패치가 이루어질 수 있다며 공개하지 않았다.

체코의 사이버 보안 소프트웨어 회사인 어베스트(Avast)가 도넥스(DoNex) 랜섬웨어의 키 재사용 취약점을 이용한 복호화 툴을 공개했다. Avast 는 3 월부터 비공개로 피해자들을 지원하기 시작했으며, 7 월에는 더 이상 DoNex 랜섬웨어의 활동이 감지되지 않아 복호화 툴을 공개했다. DoNex 랜섬웨어는 여러 차례 리브랜딩된 그룹으로, 2022 년 4 월 뮤즈(Muse) 랜섬웨어로 시작해 2022 년 11 월에는 fake LockBit 3.0 을 사용했으며, 2023 년 5 월에는 다크레이스(DarkRace)로 이름을 변경했다. 이 후 2024 년 3 월 DoNex 랜섬웨어로 리브랜딩 됐지만, 5 건의 피해자 게시 이후 추가적인 활동이 확인되지 않았으며, 4 월에는 다크웹 유출 사이트마저 비활성화됐다.

[2] ESXi: VMware 에서 개발한 호스트 컴퓨터에서 다수의 운영체제를 동시에 실행시킬 수 있는 UNIX 기반의 논리적 플랫폼

[3] 빌더(Builder): 환경 설정을 통해 원하는 기능으로 이루어진 랜섬웨어를 만들 수 있는 랜섬웨어 제작 툴

■ 랜섬웨어 뉴스

infosec

CrowdStrike 패치/업데이트로 위장한 악성코드 배포

- 미국의 사이버 보안 기술 회사 CrowdStrike의 7월 19일 업데이트로 시스템 충돌 및 블루스크린 증상 발생
- 업데이트 혹은 패치로 위장한 문서에 악성코드를 함께 첨부하여 배포
- 핵티비스트 Handala는 PDF 파일에 Wiper 다운로드 링크를 첨부하여 Wiper 배포

BrainCipher 그룹 다크웹 유출 사이트에 복호화 키 공개

- 6월 20일에 공격한 인도네시아 국가 임시 데이터 센터에 대한 복호화 키
- 정치적 동기 때문에 공격한 것이 아니라 금전을 대가로 한 침투 테스트라고 주장
- 수사기관의 외압으로 공개하는 것이 아니라 이번에만 자발적으로 복호화 키를 공개하는 것이라 주장

해킹 포럼 BreachForums에 한국 기관 데이터 판매 글 3건 게시

- BreachForums에서 활동하는 IntelBroker가 한국 기관 데이터 판매 글을 3건 게시
- 언급된 기관 명은 "Korean Policy Force", "Korean Government Agency", "Korean Critical Government Agency"
- 별도로 공개된 샘플 데이터는 없으며, 이는 공개 시 차단돼 더 이상 접근할 수 없기 때문이라고 주장

LockBit 랜섬웨어, 다크웹 유출 사이트에 연락처 공개

- 연락 책임자로 추정되는 담당자 "Boss"의 각종 메신저 ID와 해킹 포럼 프로필을 공개
- 간결하게 용건만 하나의 메시지로 전달할 것을 요구
- 공개된 암호화 메신저 ID 및 프로필 정보는 Tox ID, XMPP, Briar ID, Ramp forum profile, Telegram ID, Signal ID

VMware ESXi 취약점(CVE-2024-37085)를 악용한 랜섬웨어 그룹

- 6월 25일 공개된 ESXi 8.0 U3 버전에서 발견된 인증 우회 취약점으로, 가상 환경 전체에 대한 관리자 권한 획득 가능
- 취약점 악용에는 높은 권한이 필요하지만, 다수의 그룹이 이미 이를 악용
- Storm-0506, Storm-1175, Octo Tempest, Manatee Tempest가 Akira, BlackBasta 랜섬웨어 배포에 사용

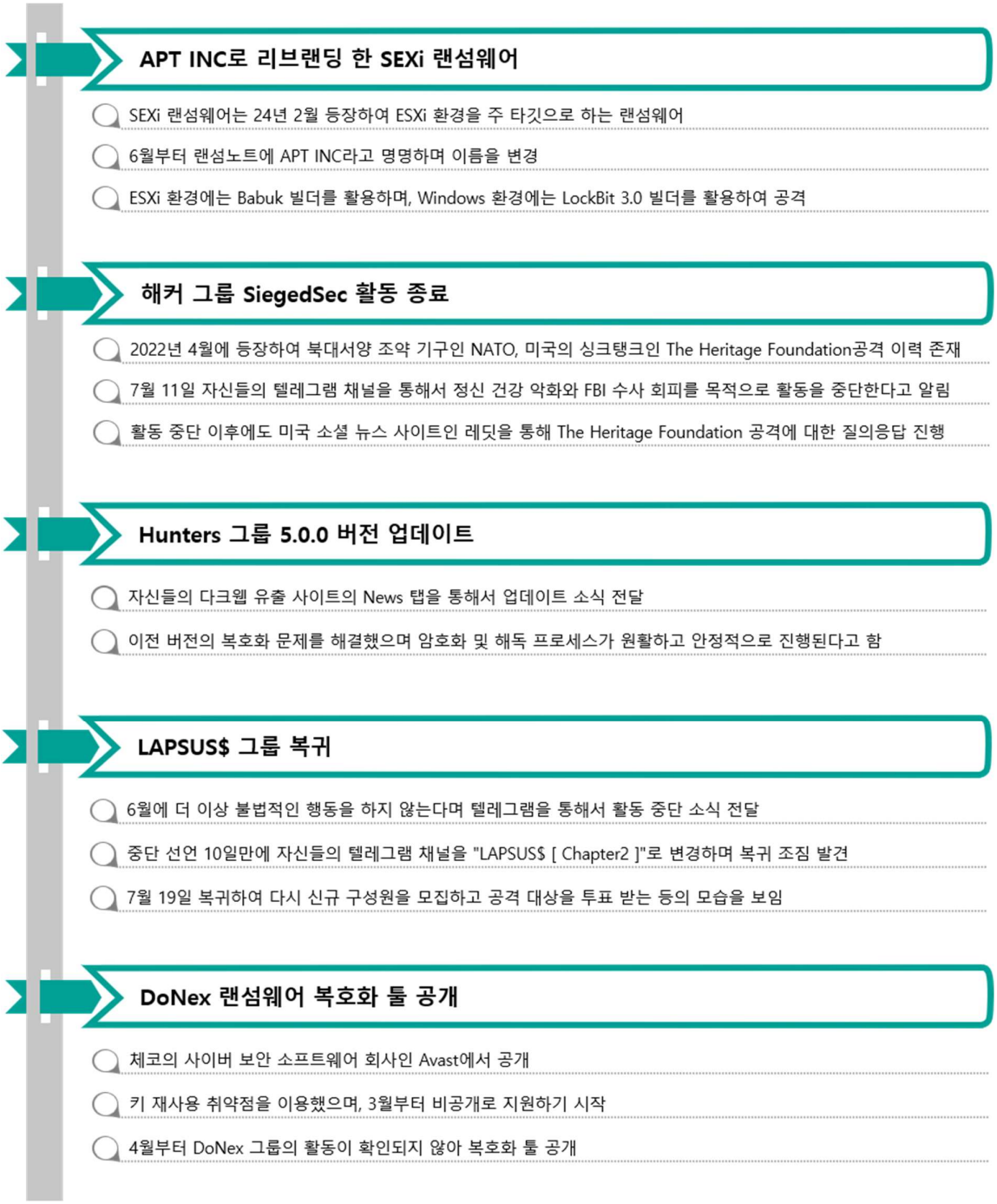

APT INC로 리브랜딩 한 SEXi 랜섬웨어
SEXi 랜섬웨어는 24년 2월 등장하여 ESXi 환경을 주 타깃으로 하는 랜섬웨어
6월부터 랜섬노트에 APT INC라고 명명하며 이름을 변경
ESXi 환경에는 Babuk 빌더를 활용하며, Windows 환경에는 LockBit 3.0 빌더를 활용하여 공격
해커 그룹 SiegedSec 활동 종료
2022년 4월에 등장하여 북대서양 조약 기구인 NATO, 미국의 싱크탱크인 The Heritage Foundation공격 이력 존재
7월 11일 자신들의 텔레그램 채널을 통해서 정신 건강 악화와 FBI 수사 회피를 목적으로 활동을 중단한다고 알림
활동 중단 이후에도 미국 소셜 뉴스 사이트인 레딧을 통해 The Heritage Foundation 공격에 대한 질의응답 진행
Hunters 그룹 5.0.0 버전 업데이트
자신들의 다크웹 유출 사이트의 News 탭을 통해서 업데이트 소식 전달
이전 버전의 복호화 문제를 해결했으며 암호화 및 해독 프로세스가 원활하고 안정적으로 진행된다고 함
LAPSUS$ 그룹 복귀
6월에 더 이상 불법적인 행동을 하지 않는다며 텔레그램을 통해서 활동 중단 소식 전달
중단 선언 10일만에 자신들의 텔레그램 채널을 "LAPSUS$ [Chapter2]"로 변경하며 복귀 조짐 발견
7월 19일 복귀하여 다시 신규 구성원을 모집하고 공격 대상을 투표 받는 등의 모습을 보임
DoNex 랜섬웨어 복호화 툴 공개
체코의 사이버 보안 소프트웨어 회사인 Avast에서 공개
키 재사용 취약점을 이용했으며, 3월부터 비공개로 지원하기 시작
4월부터 DoNex 그룹의 활동이 확인되지 않아 복호화 툴 공개

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

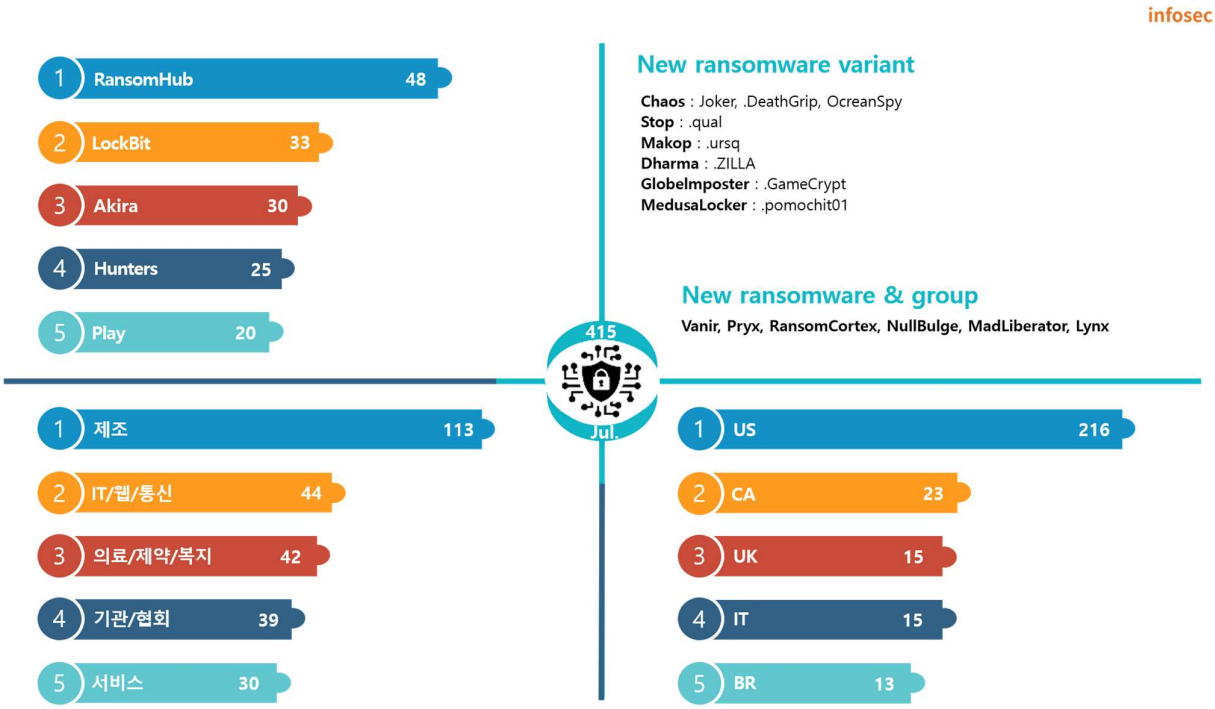


그림 2. 2024 년 7 월 랜섬웨어 위협 현황

새로운 위협

7 월에는 여러 신규 랜섬웨어 그룹이 등장했으며, 활동을 중단했던 그룹이 다시 활동을 재개하기도 했다. 랩서스(LAPSUS$) 그룹은 지난 6 월 텔레그램 채널을 통해서 활동 중단 소식을 전했으나, 한 달 만에 다시 복귀해 신규 구성원 모집과 다음 공격 대상을 투표하는 등 활동을 이어가고 있다.

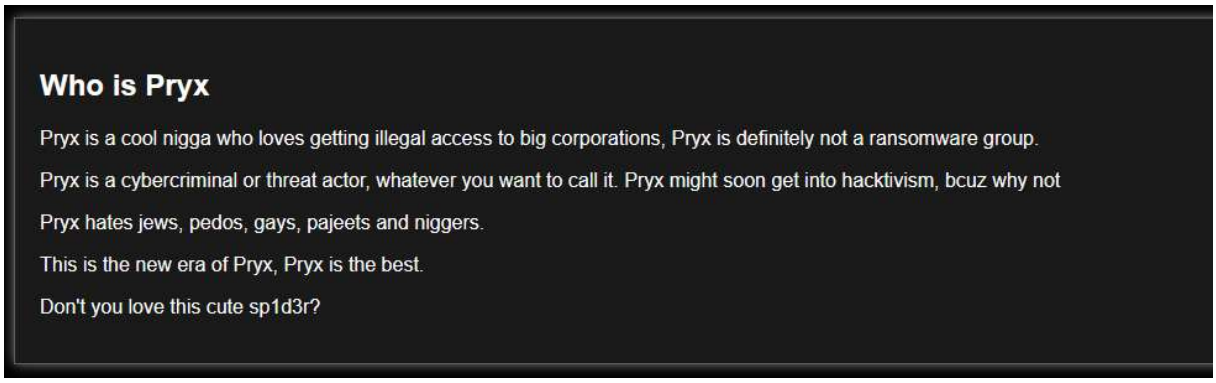


그림 3. Pryx 그룹 소개

7 월 새롭게 등장한 Pryx 그룹은 두 건의 피해자를 게시했다. 이들은 다크웹 유출 사이트에 자신들이 랜섬웨어 그룹이 아니며, 핵티비스트가 될 수도 있다고 명시했다. 또한 다크웹 유출 사이트에는 댓글을 남길 수 있는 페이지가 있으며, 데이터 유출 게시글 외에도 아랍의 봄과 2023 년 프랑스 폭력 시위와 같은 정치적인 내용의 게시글도 확인된다. 이로 인해 이들이 밝힌 바와 같이 랜섬웨어보다는 사회적·정치적 목적의 핵티비즘 성격이 강하게 보인다.

그림 4. 그룹별 다크웹 유출 사이트 (상: Vanir, 하: Akira)

Vanir 랜섬웨어의 다크웹 유출 사이트는 아키라(Akira) 랜섬웨어 그룹과 유사한 명령어 쉘 디자인을 사용하고 있으며, 명령어를 입력해 다른 페이지로 이동하는 방식도 매우 유사하다. 현재까지 총 세 건의 피해자를 게시했으며, 다크웹 유출 사이트에서 파트너를 모집하는 글도 확인됐다.

Madliberator 그룹은 7 월에만 8 건의 피해자를 게시했다. 피해자 수는 많지 않지만 제조업, 금융업, 기관, 의료, 유통 등 다양한 산업 분야에 걸쳐 피해자를 게시했다. 이 외에도 신규 Lynx 그룹은 2 건의 피해자를 게시했으며, 핵티비스트 널벌지(NullBulge)는 인도 유튜버 ChiefShifter 의 디스코드 데이터와 미국의 종합 미디어 기업 디즈니의 내부 협업 도구 데이터 1.2TB 를 공개하기도 했다.

그림 5. RansomCortex 다크웹 유출 사이트

마지막으로, 7 월 11 일 등장한 신규 RansomCortex 그룹은 등장과 함께 의료 업계와 관련이 있는 피해자 4 건을 게시했다. 그러나 8 월 1 일 기준으로 다크웹 유출 사이트의 모든 데이터가 내려갔고, 사이트의 타이틀이 “Offline”으로 변경되며 추가적인 활동은 확인되지 않고 있다.

Top5 랜섬웨어

그림 6. 산업/국가별 주요 랜섬웨어 공격 현황

랜섬허브(RansomHub) 그룹은 7 월에만 전체 활동량의 32%에 해당하는 48 건을 게시하며 활발한 활동을 보이고 있다. 지난 3 월 블랙캣(BlackCat/Alphv)의 엑시트스캠(Exit Scam) [4] 이후, BlackCat(Alphv)의 파트너들이 RansomHub 에 합류하면서 3 월부터 활동량이 꾸준히 증가하고 있다. 6 월에는 국내 건축 사무소를 공격했으며, 7 월에는 미국 플로리다 주의 보건부를 공격했다. 또한 7 월에는 랜섬웨어에 일부 기능이 추가된 신규 버전이 발견되기도 했다. RansomHub 에 대한 상세한 분석 내용은 SK 쉴더스의 2024 년 2 분기 랜섬웨어 동향 보고서인 “KARA 랜섬웨어 동향 보고서 2024 2Q”에서 확인할 수 있다.

[4] 엑시트스캠(Exit Scam): 계열사에게 수수료를 지급하지 않거나 랜섬웨어 피해자에게 돈을 지불 받고 파일 복구를 해주지 않은 채 사라지는 사기 행위

LockBit 랜섬웨어 그룹은 지난달 12건으로 상대적으로 낮은 피해 건수를 기록했지만, 7월에는 다시 활동량을 늘리며 33 건의 피해자를 게시했다. 하지만 7 월에는 LockBit 랜섬웨어 공격에 연루된 2명이 유죄를 인정했으며, 다크웹 유출 사이트가 간헐적으로 접속이 불가능하거나 테스트 게시글이 빈번히 올라오는 등 여전히 불안한 모습을 보이고 있다.

Akira 그룹은 2023 년 4 월에 등장해 활동을 이어가고 있으며, 7 월에는 VMware ESXi 인증 우회 취약점인 CVE-2024-37085 을 이용한 정황이 발견됐다. 이들은 이번 달에 캐나다의 협동조합연합회인 Federated Co-operatives Limited 를 공격해 식료품 재고 문제와 카드 잠금 중단 등의 문제를 발생시켜 연합원 소매점 운영에도 영향을 미쳤다. 또한, 금융 기관인 Financoop 을 공격해 약 20GB 의 재무 정보 및 내부 데이터를 탈취했으며, 원유 및 정제 석유 운송 서비스 기업인 Heidmar 도 공격했다.

헌터스(Hunters) 랜섬웨어 그룹은 다크웹 유출 사이트를 통해 암호화 및 복호화 도구가 5.0.0 버전으로 업데이트되었음을 전했다. 이는 이전 버전의 문제를 모두 해결한 버전으로, 암호화 및 복호화가 좀 더 원활하게 진행될 것이라고 한다. 이들은 미국의 재활 의료 서비스 제공 업체인 Northeast Rehabilitation Hospital Network 를 공격해 약 410GB 의 병원 운영 자료와 환자 정보를 탈취했다. 또한, 케냐의 도시 도로 당국인 Kenya Urban Roads Authority 를 공격해 개인 식별 정보, 재무 문서 및 고객 데이터를 포함해 약 18GB 의 데이터를 탈취하기도 했다.

플레이(Play) 랜섬웨어 그룹의 경우 활동 기간 중 전체 공격의 61%가 미국 소재 기업을 대상으로 하고 있다. 특히, 지난 7 월에는 모든 공격이 미국을 대상으로 이루어졌다. 최근 Linux 환경에서 VMware ESXi 환경을 암호화하는 기능을 가진 랜섬웨어 변종이 발견됐다. 이를 이용해서 VM 디스크나 구성 파일을 손상시키거나 가상머신 파일을 암호화할 수 있으며, 기존보다 더 많은 플랫폼에 영향을 미칠 수 있어 주의가 필요하다.

■ 랜섬웨어 집중 포커스

FOG 랜섬웨어 개요

출처: FOG 랜섬웨어 데이터 유출 사이트

2024 년 5 월부터 포착된 FOG 랜섬웨어는 활동 초기에 별도의 다크웹 유출 사이트가 확인되지 않았고, 랜섬노트에 기재된 다크웹 채팅 페이지를 통해 피해자와 협상하는 방식을 사용했다. 그러나 7 월 17 일, 피해자가 7 건이 게시된 다크웹 유출 사이트가 발견됐으며, 이후 4 건을 추가로 게시하면서 총 11 건의 피해자를 게시했다.

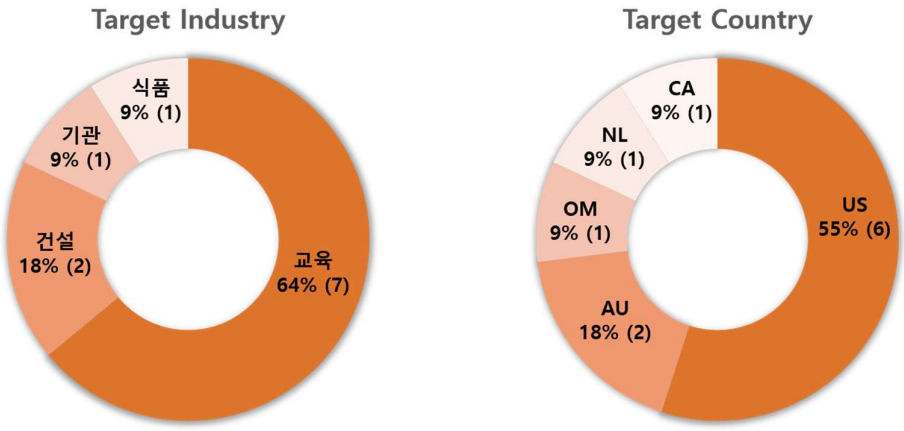


그림 7. FOG 랜섬웨어 공격 통계

다크웹 유출 사이트에 게시된 피해자는 주로 교육기관으로 확인됐다. 11 건의 피해자 중 7 건이 교육기관이며, 호주의 질롱 루터란 대학, 오만 독일 기술 대학교, 미국 텍사스 오데사 대학, 미국 위치타 주립 대학교 응용과학 및 기술 캠퍼스 등 대학뿐만 아니라 미국 일부 지역의 학군도 포함되어 있다.

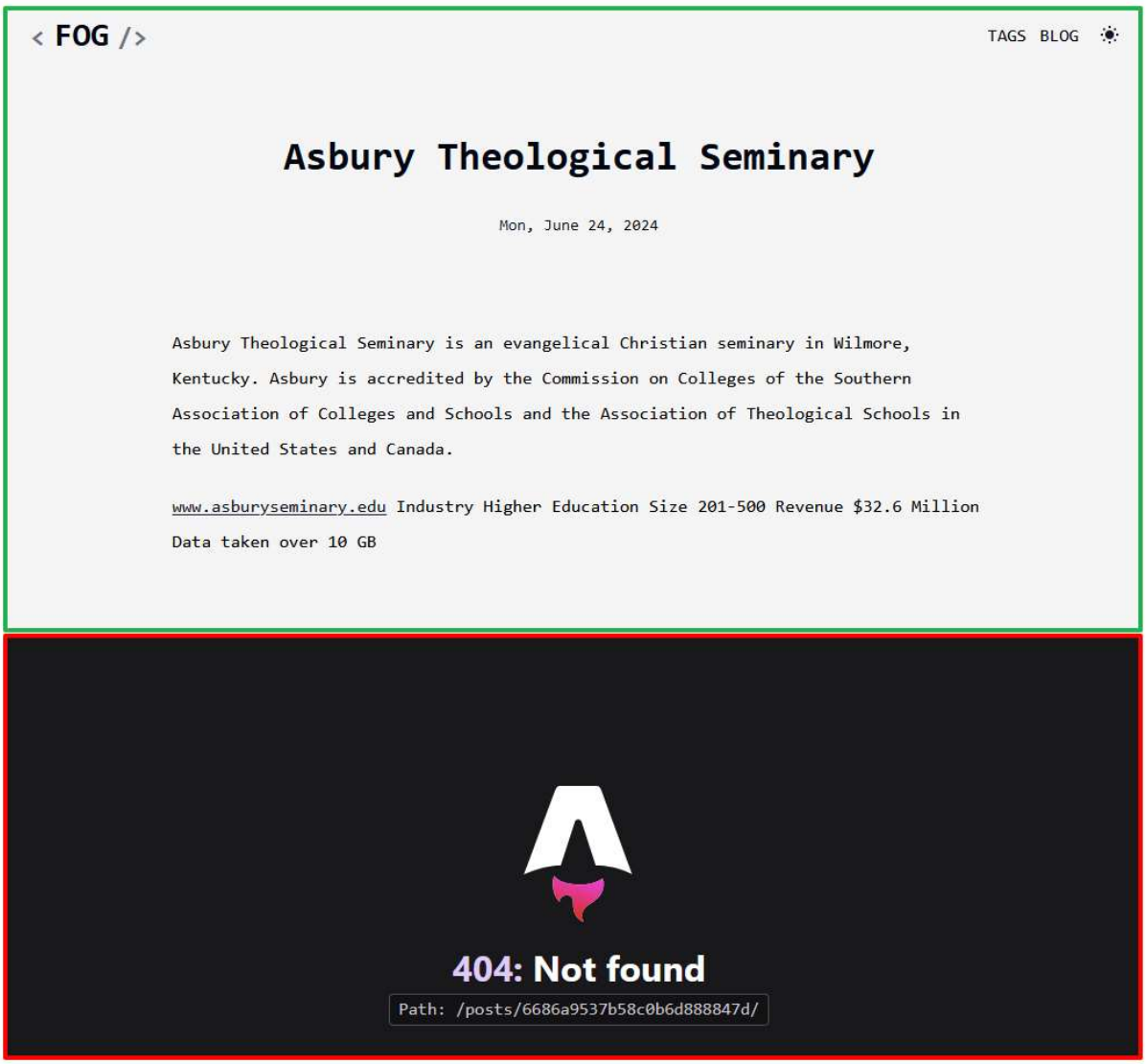


그림 8. FOG 랜섬웨어 데이터 유출 사이트의 게시글 열람 화면 (상: 열람 가능한 게시글, 하: 열람 불가능한 게시글)

FOG 랜섬웨어 다크웹 유출 사이트는 7 월 17 일에 발견된 이후로 꾸준히 피해자가 게시되고 있지만, 대부분의 게시글을 열람할 수 없는 상태다. 7 월 30 일을 기준으로 11 건의 게시글 중 1 건은 삭제된 상태이며, 2 개의 게시글만 열람할 수 있고 나머지 8 개의 게시글은 페이지가 존재하지 않는다는 에러 페이지로 안내된다. 또한, 정상적으로 접근이 가능한 2 개의 게시글에도 별도의 샘플 데이터나 공개된 데이터는 존재하지 않는다. 다크웹 유출 사이트가 원활하게 운영되지 않는 점은 운영 미숙이나 채팅 페이지에서 협상이 결렬된 경우에만 게시글을 수정하는 방식 등 여러 가능성이 있으므로 지속적인 관찰이 필요하다.

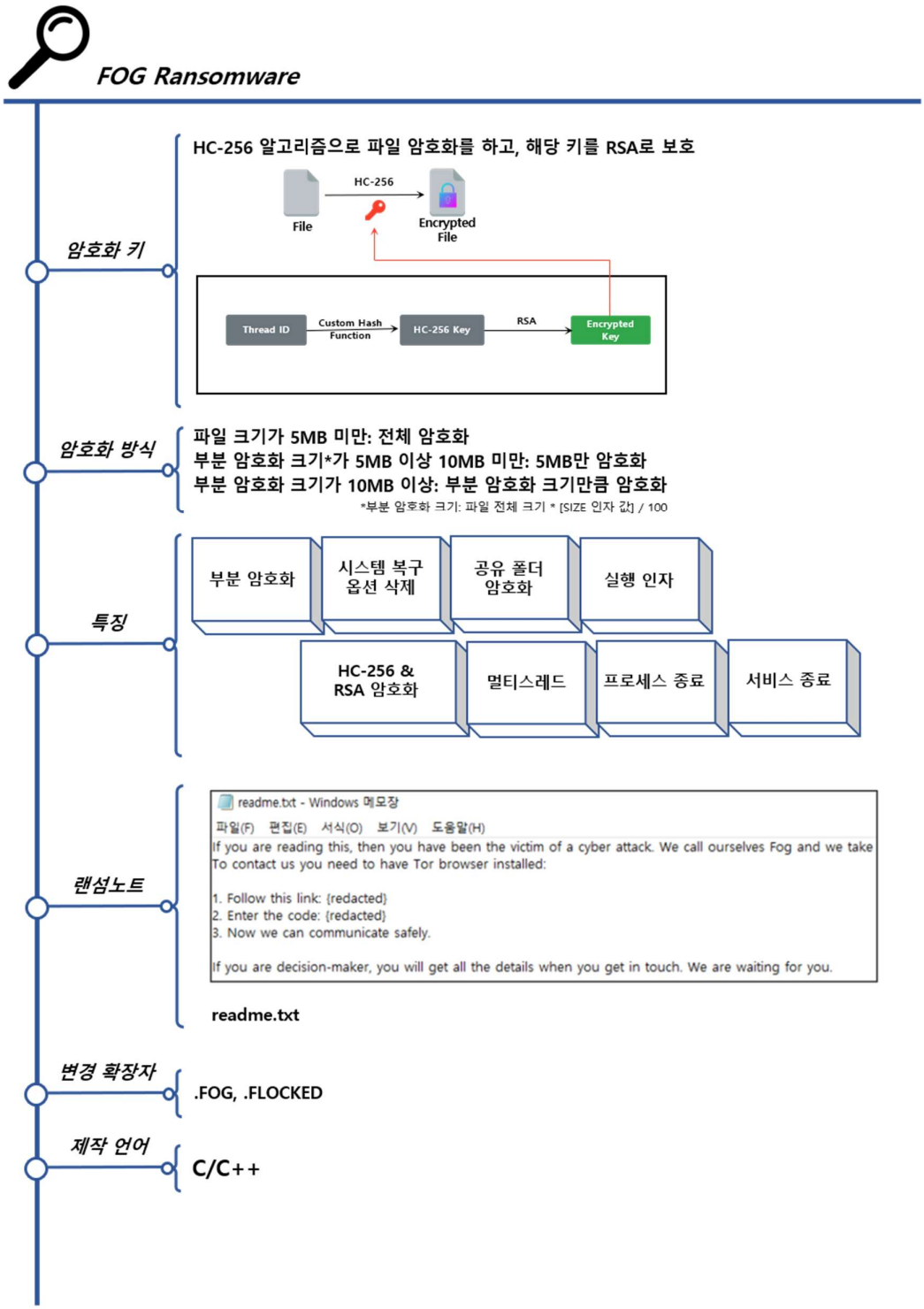


그림 9. FOG 랜섬웨어 개요

FOG 랜섬웨어 전략

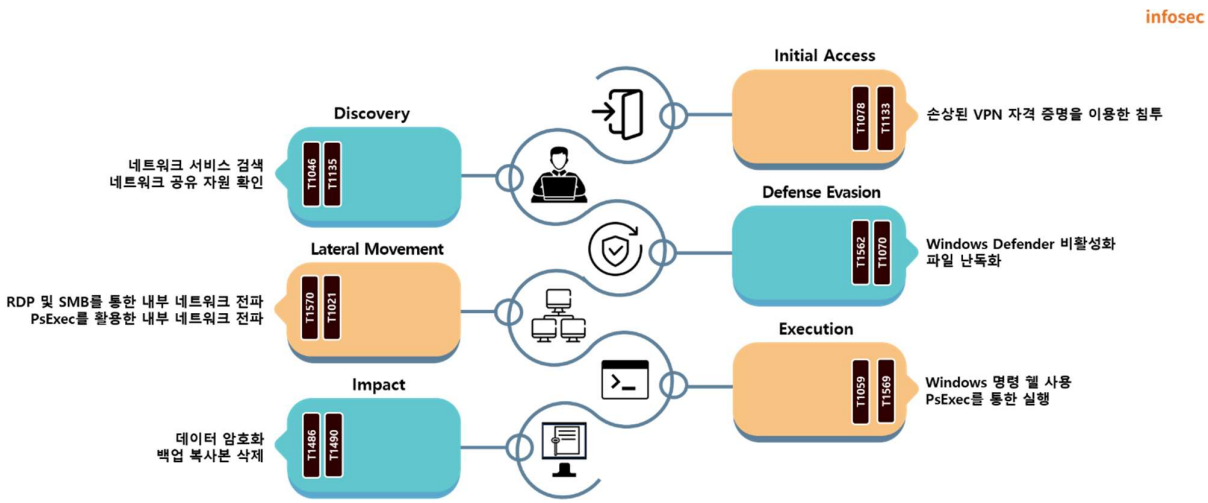


그림 10. FOG 랜섬웨어 공격 전략

FOG 랜섬웨어는 손상된 VPN[5] 자격증명을 이용해 피해자 네트워크에 침투하는 방식을 사용한다. 최초 침투 후 대상 시스템에서 네트워크 서비스를 검색하고 추가적인 악성 행위가 탐지되지 않도록 Windows Defender 를 비활성화 한다. 이후 확인된 내부 네트워크에 RDP[6] 및 SMB[7]를 통해 내부 확산을 시도하고, PsExec[8]를 통해서 페이로드[9]를 배포 및 실행한다. 배포되는 페이로드에는 Hyper-V[10] 환경의 VMDK[11] 파일을 암호화하고 Veeam[12]의 저장소 백업을 삭제하는 PowerShell 스크립트와 로컬 시스템 및 네트워크 공유 자원을 암호화하는 랜섬웨어 페이로드가 포함되어 있다.

FOG 랜섬웨어는 여러 실행 인자를 입력 받아 실행할 수 있다. RSA 공개키, 암호화 예외 대상, 종료 대상 프로세스 및 서비스 목록 등 랜섬웨어 실행에 필요한 설정 값을 복호화하기 위한 키 값을 "-ID" 인자로 전달해야 정상적으로 동작한다. 이 외에도 각종 기능을 활성화 혹은 비활성화 할 수 있는 실행 인자는 아래 표와 같다.

[5] VPN(Virtual Private Network): 인터넷 상에서 개인 정보를 보호하고 지역 제한을 우회하기 위해 사용하는 가상의 보안 네트워크

[6] RDP(Remote Desktop Protocol): 다른 컴퓨터를 원격으로 제어할 수 있도록 해주는 프로토콜

[7] SMB(Server Message Block): Windows 환경에서 파일이나 디렉토리 및 주변 장치들을 공유하는데 사용되는 메시지 형식

[8] PsExec: 다른 시스템에 별도의 소프트웨어를 설치하지 않고 프로세스를 원격으로 실행할 수 있게 해주는 명령줄 도구

[9] 페이로드(payload): 컴퓨터 시스템에 침투, 변경 또는 기타 방식으로 손상을 입히도록 설계된 코드

[10] Hyper-V: Windows 환경에서 여러 운영체제를 실행시킬 수 있도록 하는 가상화 도구

[11] VMDK(Virtual Machine Disk): 가상 환경에서 사용하는 가상 하드 디스크 드라이브

[12] Veeam: Windows 운영체제의 가상화 도구인 Microsoft Hyper-V 가상 환경에서 사용할 수 있는 백업 앱

인자	설명
-NOMUTEX	뮤텍스[13] 생성 기능 비활성화
-LOG	랜섬웨어 시작 로그를 C:₩ProgramData₩lock_log.txt 에 저장
-TARGET {PATH}	지정된 경로에 있는 파일만 암호화
-ID {KEY}	랜섬웨어가 사용하는 각종 설정 값을 복호화 하는데 필요한 키
-CONSOLE	파일 암호화 로그를 출력하는 콘솔 창 생성
-PROCOFF	프로세스 종료 기능 비활성화
-UNCOFF	네트워크 공유 자원 암호화 기능 비활성화
-SIZE {INT}	전체 파일 중 암호화를 진행할 비율 값 {int}% (기본값: 15)

표 1. FOG 랜섬웨어 실행 인자

FOG 랜섬웨어는 디버깅[14]을 목적으로 로그 파일을 생성한다. 별도의 실행 인자에 따라서 2 개의 로그를 추가적으로 생성할 수 있다. 랜섬웨어 실행 시 각 기능별 시작 메시지와 종료 메시지, 실행 결과, 에러 메시지 등 디버깅을 목적으로 사용하는 로그를 "C:₩ProgramData₩DbgLog.sys" 경로에 저장한다. 이 외에도 "-LOG" 인자를 사용하면 랜섬웨어 시작 시간이 적힌 로그 파일을 "C:₩ProgramData₩lock_log.txt" 경로에 저장하며, "-CONSOLE" 인자를 입력하면 파일 암호화 과정 중에 암호화 대상 파일 이름을 별도의 콘솔 창에 출력하며 현재 어떤 파일을 암호화하는지 확인할 수 있다.

```
2024-07-26 오전 10:28:11 [+] Defined mutex name: jBgB4ZHxUhNdJL9mz61WFXxI0GUXPAxw
2024-07-26 오전 10:28:11 [=] Decrypting json config
2024-07-26 오전 10:28:11 [=] Checking mutex...
2024-07-26 오전 10:28:11 [!] Skip mutex check by -nomutex param.
2024-07-26 오전 10:28:24 [+] JSON config loaded successfully
2024-07-26 오전 10:28:24 [=] Init prgn data...
2024-07-26 오전 10:28:25 Found disk # 1 (C:\), type: 1
2024-07-26 오전 10:28:25 Uknonwn DrvType (5) of root: D:\, skipped
2024-07-26 오전 10:28:25 [=] thread 14168 created
2024-07-26 오전 10:28:25 [=] thread 9100 created
2024-07-26 오전 10:28:25 [=] thread 5324 created
```

그림 11. DbgLog.sys 로그

FOG 랜섬웨어는 실행에 필요한 설정 값이 암호화되어 있다. 실행 인자 "-ID" 로 전달된 값을 커스텀 해시 알고리즘을 이용해 512bit 크기의 키로 만든 후, HC-256 알고리즘으로 설정 값을 복호화 한다. 복호화 된 설정 값은 힙 메모리 영역에 저장되며, 정상적으로 복호화 된 경우에만 랜섬웨어가 종료되지 않고 실행된다. FOG 랜섬웨어가 사용하는 각 설정 값의 역할은 아래 표와 같다.

[13] 뮤텍스(Mutex): 멀티스레드에서 하나의 자원에 여러 스레드가 동시에 접근하는 것을 방지하기 위한 기법

[14] 디버깅(Debugging): 프로그램 개발 단계 중에 발생하는 시스템의 오류를 찾아내 수정하는 과정

설정값	설명
PathStopList	암호화 예외 디렉토리
FileMaskStopList	암호화 예외 파일 확장자
ShutdownProcesses	프로세스 종료 대상 리스트
ShutdownServices	서비스 종료 대상 리스트
RSAPubKey	파일 암호화 키 보호에 사용되는 RSA 공개키
LockedExt	암호화 파일 변경 확장자
NoteFileName	랜섬노트 파일명
NoteFileContents	랜섬노트 내용

표 2. FOG 랜섬웨어 설정 값

파일을 암호화하기 전에, 각종 프로세스와 서비스를 종료시킨다. 이때 종료 대상은 복호화 된 설정 값 중 “ShutdownProcesses", “ShutdownServices” 리스트에 저장되어 있다. 만일 "-PROCOFF” 인자를 입력했다면, 암호화 이전에 프로세스 및 서비스 종료를 생략하고 바로 파일 암호화를 시작한다. 파일 암호화는 기본적으로 로컬 드라이브와 네트워크 공유 자원을 모두 탐색해 암호화 예외 디렉토리와 예외 확장자를 가진 파일을 제외한 모든 파일을 암호화한다. 랜섬웨어 실행 시 "-UNCOFF” 인자를 사용하면 네트워크 공유 자원은 암호화하지 않으며 “-Target” 인자를 사용하면 전체 드라이브를 암호화하는 것이 아니라 인자와 함께 입력한 경로만 암호화한다.

파일 암호화는 파일 크기와 “-SIZE” 인자 값을 통해서 부분 암호화 여부를 결정한다. 입력한 “-SIZE” 값을 파일 전체 크기의 퍼센트(%)로 계산해 부분 암호화 크기로 사용한다. 예를 들어 “-SIZE 20”으로 입력하면, 전체 파일 크기의 20%를 부분 암호화 크기로 사용한다. 파일의 크기가 5MB 보다 작은 경우에는 파일 전체를 암호화하고, 그 외의 경우에는 부분 암호화 방식을 사용한다. 부분 암호화도 크기에 따라서 방식에 차이가 있는데, 앞서 계산된 부분 암호화 크기가 5MB 이상 10MB 미만인 경우에는 파일의 5MB 만 암호화하고, 10MB 이상인 경우에는 계산된 부분 암호화 크기만큼 암호화를 진행한다. HC-256 알고리즘을 이용해 파일 암호화를 진행하며, 암호화에 사용된 키는 설정 값에 저장되어 있는 RSA 공개키를 이용해 보호한다.

이 외에도 Windows 명령어를 사용해 디스크 백업 복사본과 휴지통 데이터를 모두 삭제해 사용자의 임의 복구를 방지한다.

FOG 랜섬웨어 대응방안

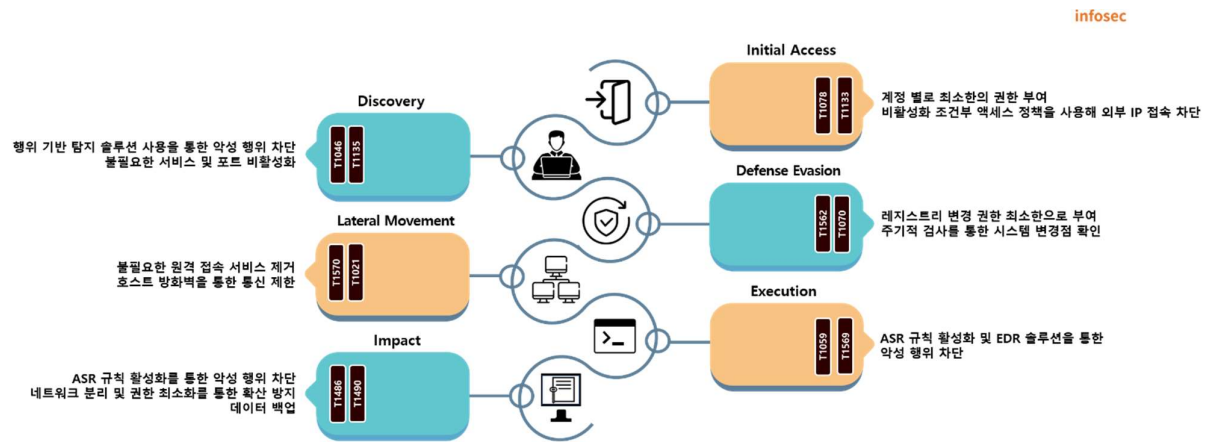


그림 12. FOG 랜섬웨어 대응방안

FOG 랜섬웨어는 초기 침투를 위해 손상된 VPN 자격증명을 이용한다. 이를 방지하기 위해서 각 계정 별로 최소한의 권한을 부여하거나, 비활성화 조건부 액세스 정책을 사용해 규정을 준수하지 않는 장치나 외부 IP 에서 로그인하지 못하도록 제한해야 한다. 또한, 원격으로 사용 가능한 서비스 중 불필요한 서비스는 비활성화하거나 차단하고, 주기적으로 계정을 점검 및 감사하여 필요하지 않은 계정은 비활성화하거나 제한하는 등 관리가 필요하다.

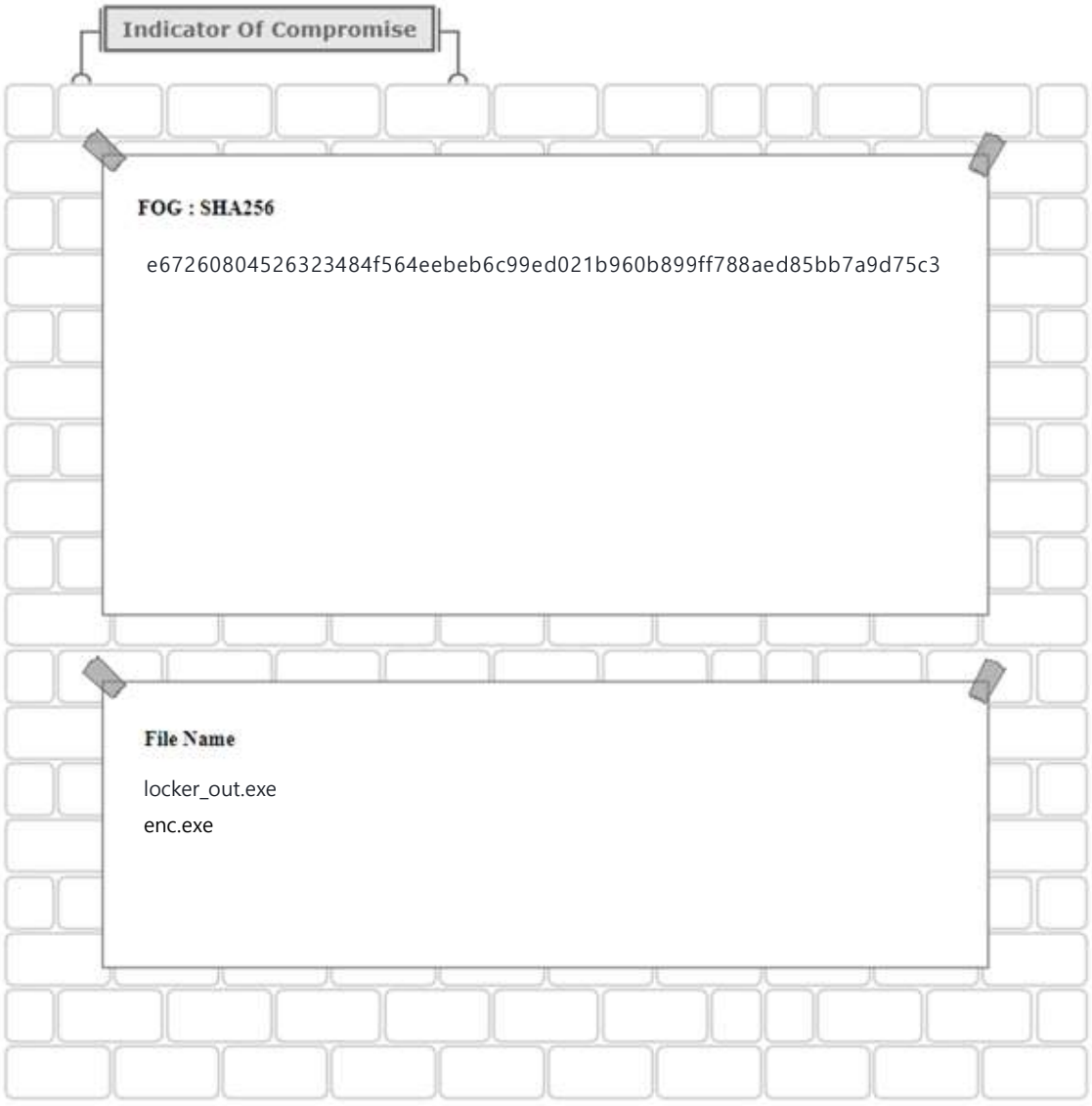
FOG 는 VPN 을 이용해 초기 침투 후 내부 네트워크에 추가적으로 확산하기 위해 공유 자원이나 각종 네트워크 서비스를 탐색한다. 네트워크 공유 자원을 열거할 수 있는 사용자를 제한하기 위해 Windows 그룹 정책을 수정해야 한다. 이 외에도 불필요한 서비스나 포트를 사전에 비활성화해 탐색되지 않도록 할 수 있다. 또한, 내부 확산을 위해 SMB, RDP, PsExec 등을 이용하므로 비정상적인 통신을 제한하기 위해 호스트 방화벽을 사용하는 것도 하나의 방법이다.

FOG 는 침투한 내부 네트워크에는 VM 환경을 손상시키기 위한 PowerShell 스크립트와 랜섬웨어 페이로드를 배포한다. 이를 방지하기 위해 ASR[15] 규칙을 활성화하거나 EDR[16] 솔루션을 활용해 악성 행위를 차단할 수 있다.

마지막으로, FOG 랜섬웨어는 로컬 디스크뿐만 아니라 네트워크 공유 파일도 암호화하기 때문에 네트워크 공유 자원의 접근 권한을 최소화하거나 비활성화하여 외부 리소스에 접근할 수 없도록 해야 한다. 또한, 사용자가 임의로 복구하는 것을 방지하기 위해 백업 복사본을 삭제하는 기능이 있으므로, 별도의 네트워크나 저장소에 데이터를 소산 백업해야 한다.

[15] ASR(Attack Surface Reduction): 공격자가 사용하는 특정 프로세스와 실행 가능한 프로세스를 차단하는 보호 기능

[16] EDR(Endpoint Detection and Response): 컴퓨터와 모바일, 서버 등 단말기에서 발생하는 악성 행위를 실시간으로 감지하고 분석 및 대응하여 피해 확산을 막는 솔루션


Indicator Of Compromise
FOG : SHA256
e672608045263234 84f564eebeb6c99ed021b960b899ff788aed85bb7a9d75c3
File Name
locker_out.exe
enc.exe

■ 참고 사이트

• TrendMicro 공식 홈페이지(https://www.trendmicro.com/en_us/research/24/g/new-play-ransomware-linux-variant-targets-esxi-shows-ties-with-p.html

• Trellix 공식 홈페이지 (https://www.trellix.com/blogs/research/akira-ransomware/)

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/fake-crowdstrike-fixes-target-companies-with-malware-data-wipers/)

• Avast 공식 블로그 (https://decoded.avast.io/threatresearch/decrypted-donex-ransomware-and-its-predecessors/)

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/meet-brain-cipher-the-new-ransomware-behind-indonesia-data-center-attack/)

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/new-fog-ransomware-targets-us-education-sector-via-breached-vpns/)

• Microsoft 공식 홈페이지 (https://www.microsoft.com/en-us/security/blog/2024/07/29

/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/)

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/sexi-ransomware-rebrands-to-apt-inc-continues-vmware-esxi-attacks/)

• CrowdStrike 공식 홈페이지 (https://www.crowdstrike.com/statement-on-falcon-content-update-for-windows-hosts-kr/)